SHANA E. SCARLETT (217895)
HAGENS BERMAN SOBOL SHAPIRO LLP
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Telephone: (510) 725-3000
Facsimile: (510) 725-3001
shanas@hbsslaw.com

STEVE W. BERMAN, *pro hac vice* (application pending)
ROBERT F. LOPEZ, *pro hac vice* (application pending)
THOMAS E. LOESER (202724)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com
robl@hbsslaw.com
toml@hbsslaw.com

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ERIC THOMAS, a Texas resident, and BENJAMIN LANCASTER, a Pennsylvania resident, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

CARRIER IQ, INC., a Delaware corporation; SAMSUNG ELECTRONICS CO., LTD., a Korean company, SAMSUNG ELECTRONICS AMERICA, Inc. a New York corporation, and SAMSUNG TELECOMMUNICATIONS AMERICA, INC., a Delaware corporation,

Defendants.

No. CV 11 5819

CLASS ACTION COMPLAINT

1. VIOLATION OF FEDERAL WIRETAP ACT AS AMENDED BY THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510 *et seq.*

2. VIOLATION OF UNFAIR BUSINESS PRACTICES ACT [CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*]

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

I. INTRODUCTION

1. Defendant Carrier IQ, Inc. ("CIQ" or "Carrier IQ") created and provides software that is embedded on cellular devices manufactured by HTC Corporation; HTC America, Inc.; and Defendants Samsung Electronics, Inc.; Samsung Electronics America, Inc.; and Samsung Telecommunications America, Inc. (the "Device Manufacturers"). CIQ touts its software as a tool for cellular carriers and device manufacturers to improve end-user experience on cellular devices. CIQ claims that its software does not log key-strokes and thus does not intercept, store, and transfer consumer's electronic communications to third parties, *i.e.*, cellular carriers and device manufacturers.

2. In truth and fact, however, CIQ software does log keystrokes and does store and transmit to third parties detailed information, including the content of user messages sent and received.

3. Consumers using devices equipped with CIQ software are not notified that the software is actively running on their devices and have no idea that, and give no consent for, their private communications to be intercepted, stored, and transmitted to third parties.

4. By embedding the CIQ software in cellular and other devices that are sold to consumers whose electronic communications are then intercepted, stored, and transmitted by way of that software, Defendant CIQ and the Defendant Device Manufacturers engage in direct violations of federal wiretap law, as well as applicable state law.

5. Through this action, Plaintiffs seek to stop Defendants' unauthorized and illegal interception of electronic communications and to recover damages and other relief prescribed by law.

II. JURISDICTION

6. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 in that Plaintiffs allege violations of federal law, namely the Federal Wiretap Act as amended by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* The Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a).

7. This Court has personal jurisdiction over the Defendants in this action by way of the fact that Defendants are licensed to do business in the state of California or otherwise conduct business in the state of California.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) inasmuch as unlawful practices are alleged to have been committed in this federal judicial district and Defendants reside or regularly conduct business in this district.

9. Intradistrict assignment: assignment to the San Jose division of this Court is appropriate because Defendant CIQ is a California corporation that has its headquarters in Mountain View, Santa Clara, California, which is located in this division of the Northern District of California. Also, it is believed and therefore alleged that many members of the proposed class reside or do business in the San Jose division of the Northern District of California as well.

III. PARTIES

10. Plaintiff Eric Thomas resides in New Braunfels, Texas.

11. Plaintiff Benjamin Lancaster resides in Pittsburg, Pennsylvania.

12. Defendant Carrier IQ, Inc. is a Delaware corporation, headquartered in Mountain View, California, with additional offices in Chicago, Boston, London (UK) and Kuala Lumpur (Malaysia). On its website, CIQ has a running tally of the number of devices on which its software has been deployed which, as of November 30, 2011, indicated over 141 million cellular devices.

13. Defendant Samsung Electronics America, Inc. ("SEA") is a New York corporation with its principal place of business at Ridgefield Park, New Jersey. SEA has offices within the United States and California and sells its products throughout the United States, including throughout California.

14. Defendant Samsung Telecommunications America, Inc. ("STA") is a Delaware corporation with its principal place of business at Richardson, Texas. STA has offices within the United States and California and sells its products throughout the United States, including throughout California.

15. Defendant Samsung Electronics Co., Ltd. ("SEC") is a Korean company with its principal place of business at 1320-10, Seocho 2-dong, Seocho-gu, Seoul 137-857, South Korea.

SEC has offices within the United States and California and sells its products throughout the United States, including throughout California.

16. SEA, STA, and SEC are collectively referred to as "Samsung."

IV. FACTUAL BACKGROUND

A. Carrier IQ

17. On its website[1] under the heading, "Who we are," Carrier IQ states:

> Carrier IQ is the world's leading provider of Mobile Service Intelligence solutions. Founded in 2005 and with a management team steeped in the mobile telecoms industry, the company is privately held and funded by some of the leading players in the venture capital industry. Carrier IQ is headquartered in Mountain View, California with additional offices in Chicago, Boston, London (UK) and Kuala Lumpur (Malaysia). Our mission is to provide mobile carriers and device OEMs with unprecedented insight into service performance and usability and so enable them to deliver higher quality products and services to their customers.

18. Under the heading, "What we do," Carrier IQ touts its ability to track and deliver "data drawn directly from your subscribers' devices" to provide "detailed insight into the mobile experience as delivered at the handset. . . ." It states:

> Carrier IQ is the market leader in Mobile Service Intelligence solutions that have revolutionized the way mobile operators and device vendors gather and manage information from end users. With Carrier IQ's unique ability to provide detailed insight into service delivery and user experience, you can achieve your strategic goals more efficiently and effectively, based on data drawn directly from your subscribers' devices – the place where your customer actually experiences the service.
>
> The Carrier IQ solution goes beyond traditional point offerings that address a single business problem, to provide a comprehensive Mobile Service Intelligence platform which builds upon underlying customer experience data to enable all areas of your business to operate more effectively: from planning to operations, from marketing to customer care.
>
> Recognizing the phone as an integral part of a mobile service delivery, and using the device to measure key parameters of service quality and usage, the Carrier IQ solution gives you the unique ability to analyze in detail usage scenarios and fault conditions by type, location, application and network performance while providing you with a detailed insight into the mobile experience as delivered at the handset rather than simply the state of the network components carrying it.
>
> The resulting unprecedented insight allows you to manage your business directly to KPIs based on your customer's experience, not just system statistics.

[1] www.carrieriq.com/company/index.htm (last accessed November 30, 2011).

19. Acknowledging the serious implications of its interception, storage, and delivery of consumers' cellular device usage data, on the "Privacy and Security" page of its website,[2] Carrier IQ states:

> Carrier IQ enables mobile operators, mobile device manufacturers, application vendors and other participants in the Mobile Ecosystem to deliver high quality products and services, based on what you want, where you want and to work and perform the way you expect.
>
> In providing our products and services, Carrier IQ enables our customers to gather information on Mobile User Experiences. Carrier IQ's products were developed from inception to respect and protect user privacy and security. We have established "Best Practices" approach to privacy and security. Our products are designed and configured to work within the privacy policies of our end customers and include functions such as anonymization and encryption. When Carrier IQ's products are deployed, data gathering is done in a way where the end user is informed or involved.
>
> With deployment on over 130 million phones globally, we have considerable experience in protecting the privacy of the end user and doing so in a highly secure manner. Information transmitted from enabled mobile devices is stored in a secure data center facility that meets or exceeds industry best practice guidelines for security policies and procedures.
>
> Our data gathering and data storage policies are built from industry best practice. Our products allow us to address privacy & security requirements that vary country-by-country and customer-by-customer. There are a variety of techniques involved in protection of privacy and in implementation of security policy, including anonymization of certain user-identifiable data, aggregation of data and encryption of data, etc.
>
> We work in partnership with our customers to ensure compliance with their data collection and protection policies. While much of the data we gather data is already available through alternate methods, we make it more efficient and useful – aimed at improving products, services and quality for the end user.

20. However, despite CIQ's statement that "[w]hen Carrier IQ's products are deployed, data gathering is done in a way where the end user is informed or involved[,]" Plaintiffs and members of the proposed Class were not informed and had no way to know that Carrier IQ's software was capturing their keystrokes and intercepting, storing, and transmitting their electronic communications.

B. Discovery of Carrier IQ's interception of electronic communications

21. In mid-November 2011, a software developer named Trevor Eckhart published on the web his discovery of the Carrier IQ software on his HTC brand smartphone cellular device. Mr. Eckhart described the CarrierIQ software as a "rootkit," which is "software that enables

[2] www.carrieriq.com/company/privacy.htm (last accessed November 30, 2011).

continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications." (Citing *Wikipedia*.)

22. Mr. Eckhart revealed that the CarrierIQ software on his device was virtually impossible to deactivate, and that it provided no notice that it was embedded and operating and was capable of logging virtually everything he did on his device, including key strokes, numbers dialed, SMS (text) messages, and secure (HTTPS) website log-ins and search terms.[3]

23. Shortly thereafter, CIQ sent Mr. Eckhart a cease and desist letter demanding in part that he retract his description of the CIQ software as a rootkit, accusing him of copyright infringement for posting materials he found on its own website, and threatening severe legal action if he did not capitulate to its demands. In response, the Electronic Frontier Foundation ("EFF") stepped up to Mr. Eckhart's defense and countered with a letter demonstrating that CIQ's accusations were baseless and demanding that CIQ withdraw its letter and threatened legal action.[4]

24. On November 23, 2011, CIQ released a statement that provided:

> As, of today, we are withdrawing our cease and desist letter to Mr. Trevor Eckhart. We have reached out to Mr. Eckhart and the Electronic Frontier Foundation (EFF) to apologize. Our action was misguided and we are deeply sorry for any concern or trouble that our letter may have caused Mr. Eckhart. We sincerely appreciate and respect EFF's work on his behalf, and share their commitment to protecting free speech in a rapidly changing technological world.[5]

25. However, the November 23, 2011, CIQ statement also provided:

> We would like to take this opportunity to reiterate the functionality of Carrier IQ's software, what it does not do and what it does:
>
> - Does not record your keystrokes.
> - Does not provide tracking tools.
> - Does not inspect or report on the content of your communications, such as the content of emails and SMSs.
> - Does not provide real-time data reporting to any customer.

[3] Eckhart's initial publication can be found at http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/ (last accessed November 30, 2011).

[4] The letter can be found at: https://www.eff.org/sites/default/files/eckhart_c%26d_response.pdf

[5] http://www.carrieriq.com/company/PR.EckhartStatement.pdf

26. Mr. Eckhart was not convinced by CIQ's denial and performed further analysis on his active device and an additional device which was no longer subscribed to a cellular service but was usable over a wi-fi connection.

27. On or about November 28, 2011, Mr. Eckhart published his further analysis in a report titled Carrier IQ Part 2.[6] His report included a 17 minute video in which he stepped through proof that the CIQ software did, in fact log his key strokes, record his SMS (text) messages, record dialed numbers, and tracked his internet use, including on HTTPS (secure) websites.

28. Mr. Eckhart's report was quickly picked up by the Internet press and broadly reported. Bryan Chafin, reporting for the *Mac Observer*, wrote:

> …the entire point of the application is to collect and send data to those servers, so it's not a great stretch to believe that every text, every search, ever button, and any and every other tap you make on your HTC Android devices, RIM BlackBerry device, and Nokia smartphones is being logged and sent to Carrier IQ and then shared with whichever company paid to have the app there in the first place.[7]
>
> As you can see in the video, Carrier IQ's claim that the company is not, "recording keystrokes or providing tracking tools" is completely false.[8]

29. Andy Greenberg, reporting for *Forbes*, wrote:

> As Eckhart's analysis of the company's training videos and the debugging logs on his own HTC Evo handset have shown, Carrier IQ captures every keystroke on a device as well as location and other data, and potentially makes that data available to Carrier IQ's customers. The video he's created (below) shows every keystroke being sent to the highly-obscured application on the phone before a call, text message, or Internet data packet is ever communicated beyond the phone. Eckhart has found the application on Samsung, HTC, Nokia and RIM devices, and Carrier IQ claims on

---

[6] http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/carrieriq-part2/

[7] More specifically, affected devices are reported elsewhere on the Internet to include the Samsung Epic 4Q, as carried by Sprint; the Samsung Epic 4Q, as carried by Sprint; the Samsung Moment, as carried by Sprint; the Samsung Infuse, as carried by AT&T; and the Samsung Skyrocket, as carried by AT&T. The HTC phones are reported to include the HTC Evo, as carried by Sprint and referenced herein, as well as the Evo 3D, as carried by Sprint. Research is ongoing to determine other affected devices.

[8] http://www.macobserver.com/tmo/article/carrier_iq_collects_everything_on_android_rim_nokia_phones/

its website that it has installed the program on more than 140 million handsets.[9]

30. Mr. Greenberg, in the *Forbes* article, went on to quote Carrier IQ as recently stating in part:

> The information gathered by Carrier IQ is done so for the exclusive use of that customer, and Carrier IQ does not sell personal subscriber information to 3rd parties. The information derived from devices is encrypted and secured within our customer's network or in our audited and customer-approved facilities.

31. Russell Holly, reporting for Geek.com, wrote:

> Eckhart put together a video of him turning on an HTC Evo3D with a completely stock (provided by HTC) ROM. He demonstrates that nowhere in the startup does any mention of CarrierIQ. There's nothing indicating that this software exists on the phone. When the applications are discovered, the ability to shut the apps down the same way you would any other app in Android has been circumvented. So, you now have a series of applications that you have to be extremely knowledgeable to find, and when you do find them they *cannot be turned off*. This is demonstrated in the first five minutes of the video, and these steps can be easily re-created if you have access to LogCat on your computer.
>
> When you receive a text, the video demonstrates that the CarrierIQ software is aware of the text message and its contents before the phone notifies you that you have a message. CarrierIQ and Sprint both were adamant that the body of an SMS was not recorded, and yet we can clearly see in the video that the text contents are read and transmitted via the CarrierIQ applications. In an attempt to clear this matter up, I reached out to CarrierIQ again, who refused to comment and noted that they "are looking forwarding to our meeting with EFF this week and will continue to keep you updated."
>
> The video also demonstrates how this software records the keys that are pressed in the dialer, before a call is even made. Anytime you press a key in the dialer app, even if you just press random numbers and then close the application, that information is logged by CarrierIQ. If you place a call, that information is recorded as well, along with network strength values. This way if anything happens that would interrupt the call, your carrier can see why it happened and fix it. There's a real benefit to the CarrierIQ software, but it is clear that far more is being recorded than is necessary.
>
> ....
>
> This video has demonstrated a truly significant volume of information is being recorded. Passwords over HTTPS, the contents of your text messages, and plenty more are recorded and sent to the customers of CarrierIQ. A significant part of what was demonstrated is not included in any privacy agreement, and some of it was a direct

[9] http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases/

> contradiction of the statements that were made by these companies. It looks like we're being lied to, our information is being recorded, and there is nothing we can do about it.[10]

32. Another Android developer, Tim Schofield, extensively researched the presence of the CIQ software on multiple Android smartphone platforms. He noted that in addition to the privacy issues, the embedded CIQ software necessarily degrades the performance of any device on which it is installed. The CIQ software is *always operating and cannot be turned off.* It necessarily uses system resources, thus slowing performance and decreasing battery life. As a result, because of the CIQ software, in addition to having their private communications intercepted, Plaintiffs and Class members are not getting the optimal performance of the smartphone devices that they purchased, and which are marketed, in part, based on their speed, performance, and battery life.

33. Another harm suffered by Plaintiffs and the Class is that devices running CIQ embedded software are more vulnerable to data theft than those not running the software. CIQ software, whether it is transmitting data or not, is capable of intercepting keystrokes and incoming and outgoing communications. As a result, devices embedded with the CIQ software are vulnerable to malware, which could piggyback on the CIQ platform to intercept or capture users' private information and communications.

34. Eckhart's test showed his keystrokes being logged and messages intercepted even when his device was only connected via wi-fi to the Internet. There is no reasonable basis for a device metric application, which is what Carrier IQ calls its software, to monitor and track device actions when the device is not connected to a mobile network. This also creates a vulnerability to data theft and interception via malware transmitted or accessed through wireless connections.

C. Plaintiffs' Cellular Devices Were Embedded With Carrier IQ Software and Their Communications Were Intercepted Without Authorization

35. Plaintiff Eric Thomas owns and uses a Samsung Replenish smartphone operating on the Sprint mobile network. This device is embedded with the CIQ software. Plaintiff regularly sent and received SMS (text) messages on his Samsung device. By virtue of the unknown, not

[10] http://www.geek.com/articles/mobile/security-researcher-responds-to-carrieriq-with-video-proof-20111129/

assented-to, automatic, and unpreventable functions of the CIQ software, Plaintiff's private and personal communications have been illegally intercepted and transmitted by and to Defendants Carrier IQ and Samsung. In addition, Plaintiff has not been able to use his smartphone device at the performance levels it is capable of because the CIQ software is always operating in the background.

36. Plaintiff Benjamin Lancaster owns and uses a Samsung Galaxy S2 Skyrocket smartphone operating on the AT&T mobile network. This device is embedded with the CIQ software. Plaintiff regularly sent and received SMS (text) messages on his Samsung device. By virtue of the unknown, not assented-to, automatic, and unpreventable functions of the CIQ software, Plaintiff's private and personal communications have been illegally intercepted and transmitted by and to Defendants Carrier IQ and Samsung. In addition, Plaintiff has not been able to use his smartphone device at the performance levels it is capable of because the CIQ software is always operating in the background.

V. CLASS ALLEGATIONS

37. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of themselves and a proposed Class consisting of:

> All persons in the United States that own or owned Samsung brand telephones or other devices on which Cellular IQ software was installed or embedded.

Excluded from the proposed Class are Defendants; Defendants' affiliates and subsidiaries; Defendants' current or former employees, officers, directors, agents, and representatives; and the judge or magistrate judge to whom this case is assigned, as well as those judges' immediate family members.

38. **Numerosity:** The exact number of the members of the proposed class is unknown and is not available to the Plaintiffs at this time, but individual joinder in this case is impracticable. Based on Defendant CIQ's representation that its software is installed on over 140 million devices, it is likely that the proposed class consists of tens or hundreds of thousands, or even millions, of members.

39. **Commonality:** Numerous questions of law and fact are common to the claims of the Plaintiffs and members of the proposed class. These include:

a. Whether CIQ software installed on Plaintiffs' and proposed class members' communication devices has intercepted, and whether it has re-transmitted, Plaintiffs' and proposed Class members' SMS text messages, keystrokes, telephone numbers, and other information, all without the device owners' knowledge or consent, and whether it continues to do so.

b. Whether CIQ and the Device Manufacturers have violated the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, including the prohibition on the interception, disclosure, and use of wire, oral, or electronic communications, or otherwise, by way of the acts and omissions set forth in this complaint.

c. Whether CIQ and the Device Manufacturers have violated the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* by way of the acts and omissions set forth in this complaint.

d. Whether CIQ and the Device Manufacturers have unlawfully profited from their conduct, and whether they must disgorge profits to the Plaintiffs and members of the proposed Class.

e. Whether Plaintiffs and members of the proposed Class are entitled to statutory and other damages, civil penalties, punitive damages, restitution, and/or declaratory or injunctive relief.

40. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the proposed Class. The factual and legal bases of Defendants' liability to Plaintiffs and other members of the proposed Class are the same and resulted in injury to Plaintiffs and all of the other members of the proposed Class.

41. **Adequate representation:** Plaintiffs will represent and protect the interests of the proposed Class both fairly and adequately. They have retained counsel competent and experienced in complex class-action litigation. Plaintiffs have no interests that are antagonistic to those of the proposed Class, and their interests do not conflict with the interests of the proposed Class members they seek to represent.

42. **Predominance and Superiority:** This proposed class action is appropriate for certification. Class proceedings on these facts and this law are superior to all other available methods for the fair and efficient adjudication of this controversy, given that joinder of all members is impracticable. Even if members of the proposed Class could sustain individual litigation, that course would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex factual and legal controversies present in this controversy. Here, the class action device will present far fewer management difficulties, and it will provide the benefit of a single adjudication, economies of scale, and comprehensive supervision by this Court. Further, uniformity of decisions will be ensured.

VI. CLAIMS FOR RELIEF

COUNT I
VIOLATION OF THE FEDERAL WIRETAP ACT

43. Plaintiffs repeat and re-allege every allegation above as if set forth herein in full.

44. Plaintiffs bring this claim on their own behalf and on behalf of each member of the proposed Class described above

45. Defendants Carrier IQ and the Device Manufacturers, by way of the Carrier IQ software and their own implementing or ancillary software, have intentionally intercepted, endeavored to intercept, or procured others to intercept or endeavor to intercept, wire and/or electronic communications as described herein, all without the knowledge, consent or authorization of Plaintiffs or the Class, in violation of 18 U.S.C. § 2511(1). *See* 18 U.S.C. § 2511(1)(a).

46. Defendants Carrier IQ and the Device Manufacturers, by way of the Carrier IQ software and their own implementing or ancillary software, have intentionally disclosed, or endeavored to disclose, to other persons the contents of wire and/or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications, as described in 18 U.S.C. § 2511(1)(c). Accordingly, these Defendants have violated 18 U.S.C. § 2511(1).

47. As a result of these violations of law, Plaintiffs and the class and suffered harm and injury, including the interception and transmission of private and personal communications and the degraded performance level of the devices in question.

48. As a result of these violations of law, Defendants Carrier IQ and the Device Manufacturers are subject to civil suit, and Plaintiffs are entitled to appropriate relief, including that set forth in 18 U.S.C. § 2520(b). 18 U.S.C. § 2520(a). Such appropriate relief includes "preliminary or other equitable or declaratory relief as may be appropriate"; "damages" as described in the statute; and "a reasonable attorney's fee and other litigation costs reasonably incurred." 18 U.S.C. § 2520(b). As for damages, "the court may assess as damages whichever is the greater of—(A) the sum of the actual damages suffered by the Plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000." 18 U.S.C. § 2520(c)(2).

49. Plaintiffs, on their own behalf and on behalf of the proposed Class, seek all such appropriate relief, including but not limited to statutory damages as set forth above.

COUNT II
VIOLATION OF THE UNFAIR COMPETITION LAW
(CAL. BUS. & PROF. CODE §§ 17200 *ET SEQ.*)

50. Plaintiffs repeat and re-allege every allegation above as if set forth herein in full.

51. Plaintiffs bring this claim on their own behalf and on behalf of each member of the proposed Class described above.

52. California's Unfair Competition Law (the "UCL") defines unfair competition to include any "unlawful, unfair, or fraudulent" business act or practice. Cal. Bus. & Prof. Code §§ 17200 *et seq.*

53. Defendants engaged in "unlawful" business practices under the UCL because they violated the Federal Wiretap Act, 18 U.S.C. § 2511.

54. Defendants engaged in "unlawful" business practices under the UCL because they violated the California Consumer Protection Against Spyware Act, Cal. Bus. & Prof. Code §§ 22947-22947.6.

55. Defendants engaged in "fraudulent" business practices under the UCL because they secretly installed the CIQ software on Plaintiffs' devices, failed to disclose that the CIQ software was always operating on such devices, failed to disclose that the CIQ software was capable of intercepting Plaintiffs' private communications and, in fact intercepted such communications, and failed to disclosed that the CIQ software degraded the performance and battery life of the devices on which it was installed. Defendants' omissions and failures to disclose were "material" to Plaintiff and the class within the meaning of *In re Tobacco II Cases* 46 Cal. 4th 298, 325 (Cal. 2009).

56. Defendant engaged in "unfair" business practices under the UCL based on the foregoing, and because they violated the laws and underlying legislative policies designed to protect the privacy rights of Californians and the rights of others which are affected by companies operating out of California. In particular, Cal. Bus. & Prof. Code §§ 22947-22947.6 and the California Constitution, which provides:

> ARTICLE 1 DECLARATION OF RIGHTS
>
> SECTION 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, ***and privacy***.

57. Plaintiff and the Class were injured in fact and lost money or property as a result of these unlawful, unfair, and fraudulent business practices. In particular and without limitation, Plaintiffs did not get the performance level and battery life on their phones that they paid for because the CIQ software necessarily degraded such performance and battery life by constantly running on Plaintiffs' devices.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the following relief:

A. That the Court certify this case as a class action and appoint the named Plaintiffs to be Class representatives and their counsel to be Class counsel;

B. That the Court award them appropriate relief, to include statutory damages, as available to them under the Federal Wiretap Act, including as that set forth and described in 18 U.S.C. § 2520(b)-(c);

C. That the Court award them preliminary or other equitable or declaratory relief as may be appropriate, per 18 U.S.C. § 2520(b), or by way of other applicable state or federal law;

D. Such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the UCL violations; and

E. That the Court award them such other, favorable relief as may be available and appropriate under federal or state law, or at equity.

VIII. JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all issues so triable.

DATED: December 2, 2011

HAGENS BERMAN SOBOL SHAPIRO LLP

By _____
SHANA E. SCARLETT (217895)
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Telephone: (510) 725-3000
Facsimile: (510) 725-3001
shanas@hbsslaw.com

Steve W. Berman, *pro hac vice* (application pending)
Robert F. Lopez, *pro hac vice* (application pending)
Thomas E. Loeser (202724)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
(206) 623-7292

Attorneys for Plaintiffs and the Proposed Class